Quick Answer: How Can Organizations Use DNS to Improve Their Security Posture?

Published 8 June 2021 - ID G00723978 - 13 min read

By Analysts Craig Lawson, John Watts

Initiatives: Infrastructure Security; Cloud and Edge Infrastructure

DNS presents security and risk management leaders with some excellent opportunities to anticipate, prevent, detect and respond to prevailing threats. Organizations should implement DNS security to protect users, devices and other critical infrastructure.

Quick Answer

How can organizations use DNS to improve their security posture?

- Review the security capabilities with your existing DNS solution or services provider to identify which security use cases can be supported with the solutions already in place.

- If you don’t have a DNS service that supports security use cases, evaluate services that can provide coverage of the users, devices and critical infrastructure that matters most to you.

- Collect and analyze DNS logs for threat detection and forensics purposes using tools like your security information and event management (SIEM) or central log management tool.

- Implement DNS threat prevention and blocking capabilities — and, if possible, also monitor DNS traffic for other anomalies like data exfiltration. In some cases this might not be a new product, as this functionality may be present in one of your existing products. Ideally it can be used for enforcement as well as monitoring use cases.

More Detail

Review Your Existing DNS Solution or Services Provider to Identify Which Use Cases Can Be Supported

Because of the intrinsic nature of the function that Domain Name System (DNS) performs, it presents security and risk management leaders with opportunities to anticipate, prevent, detect and respond to prevailing threats, regardless of where the user, device or workload is located. Gartner has seen too few organizations take advantage of this opportunity. This guidance will detail compelling use cases that can be rapidly implemented.

There are several findings around DNS that are important to acknowledge:
In order to capitalize on the security capabilities of DNS, you need to be able to manage your own DNS and control DNS resolution — that is, ideally you need to “own your resolver.”

Owing your own resolver simply means that you should control what happens with DNS resolution for your users, and not solely rely on what your internet service providers (ISPs) return as the host/IP resolution answer, as these solutions are rarely built to also deliver security use cases. For example, if a host can resolve any domain/host on the internet, then you do not “own your resolver” per se, as you are not configuring it to do things like prevent resolution of malicious domains. However, DNS is a hierarchy, and there are aspects of DNS that you will never “own” either, as this is how DNS on the internet operates overall. This does not mean that other elements of DNS cannot be used for security, like logging for analysis and forensics activities. However, one of the biggest benefits of using DNS is using it to block threats to disrupt the communication between a compromised asset, implement application control and detect attacker activity.

DNS over HTTPS (DoH) is rolling out in browsers by default, which means the browser will bypass any network-level DNS and use a predetermined DNS provider. Forward-thinking organizations are blocking this at the firewall or proxy, or using Group Policy Object (GPO) settings to force browsers to respect enterprise DNS resolvers. Other organizations who use external DNS resolvers (whether internal or external) are converting to their chosen provider’s DNS over TLS (DoT) to encrypt their DNS traffic. This allows them to maintain the confidentiality of their domain resolutions. This can apply to internal DNS resolvers as well.

However, these new DNS features all support the insertion of DNS filtering. This is not a case of any organization losing visibility because of this development. Security leaders can perhaps treat this as a

---

- DNS is generally regarded as a server and networking infrastructure component and not as widely recognized for its ubiquity and utility for security use cases (such as application control, threat detection and threat prevention).
- DNS is a common service used by attackers to help compromise environments in multiple ways. Security and risk management leaders should use it tactically in response to these techniques.
- Too few end-user organizations recognize the monitoring use cases that DNS can deliver (for example, from a SIEM), such as storing, monitoring and analyzing DNS log data for security threat detection, investigation (or threat hunting), and response activities.
- DNS filtering may also be used to effectively reduce privacy risks from things like tracking websites and cookies.
good excuse to move to DNS resolver architectures that they fully control — giving them the benefit of using TLS.

An area of system configuration management (or hardening) that can be critical is ensuring that endpoints are using the appropriate DNS server in all of your build templates for servers and secure operating environments (SOEs). This also applies for end-user devices managed by UEM types of technologies (see Solution Comparison for Unified Endpoint Management [UEM] Systems and Magic Quadrant for Unified Endpoint Management). For example, it is a very common tactic for the local hosts file of machines to be modified to insert malicious host/domain names in there (or change DNS server configurations). This primarily serves as a way for threat actors to subvert DNS security or DNS monitoring capabilities to achieve their goals of compromising the host.

The COVID-19 pandemic has stunned the world and led to the quickest, and largest, remote working rollout in history (see The Risks of Remote Work: Cybersecurity). There is a significant benefit, often at little to no cost, in making some simple but fundamental changes in your security posture with DNS for both on-premises and remote workers (see A Comparison of Remote Network Access Options for Enterprise Endpoints). External recursive DNS is quite useful in this situation to achieve additional security hygiene for any device.

Create a DNS Allow List

Application allow listing is a powerful concept in cybersecurity, featuring in numerous government standards today.\(^2, 3, 4\) We are in an era where there is far more “bad” software in existence than there is “good” software. Many anti-malware vendors regularly report hundreds of millions of net new samples of malware each year now. A large majority of malware is “network-reliant.” This means that it requires network connectivity for command and control, and to move laterally throughout an environment. Almost all of this communication, like anything on a computer, requires DNS as a prerequisite. By only allowing a set list of domains to be resolved, DNS can prevent threats that use techniques like dynamic domain names and other mechanisms.

One question Gartner occasionally hears from clients is: “What about direct IP address connections that bypass DNS controls?” Typically, malware relies on multiple domain resolutions using fast flux and other dynamic domain name techniques to avoid takedowns by authorities and hosting providers. Therefore, while it does happen, malware rarely relies on direct IP address communications for command to control traffic. A relatively simple correlation rule in a SIEM can check whether names were resolved from the DNS server match with firewall connections in the same short time period. This would be a good monitoring use case to show hosts that are making direct to IP connections without making DNS requests. This highlights that a local hosts file entry could be overriding DNS for example, which would likely be worth following up on, depending on the connections being made.

Create a DNS Deny List

Deny listing has been central to cybersecurity from the very start. DNS security solutions now allow for this functionality. It is the most popular DNS security use case deployed today by Gartner clients that are
using DNS for security use cases.

A DNS service, often cloud-delivered, is configured for all relevant hosts (sometimes with the use of agents) to forward all external name resolution requests to the service. Security leaders should also look to evaluate how the solution handles dynamic domains and random domain name generation, as these are also techniques used by malware authors.

Deny listing can also be a credible way to perform application control allow listing, where only the desired services/websites are allowed to be used by that device/user. This then reduces the risk of usage of things like consumer nonsanctioned services that can risk data loss, and it prevents access to malicious sites like the ones used for phishing, botnets, and remote access trojans.

Use DNS For Host Isolation

Similar to deny lists, DNS isolation can be an effective way to perform various levels of host network isolation should it be required. However, keep in mind this is generally considered a more temporary solution until responders can get to the asset in question. In this example, a host could be infected or need active attention at a particular point in time due to its behavior. Its DNS requests can then be either fully or partially restricted to prevent it from making connections to hosts either inside or outside of the organization as security responders deem appropriate. This could be particularly useful for rapidly moving threats like ransomware — for example, malware does not function if it cannot join its botnet control fabric. It is also useful for hosts like those with embedded operating systems that do not have any type of locally running remediation or prevention controls (for example, endpoint protection platforms [EPPs] and endpoint detection and response [EDR]). Action can be taken as needed to urgently prevent or contain certain activities.

Use Machine-Readable Threat Intelligence (MRTI)

A very popular use case for threat intelligence today is to operationalize machine-readable threat intelligence to improve the threat detection, prevention and response capabilities of the numerous tools and places of enforcement and monitoring that are available to you. MRTI can also come from many different sources such as Computer Emergency Response Team (CERTs), information sharing and analysis centers (ISACs), open source, vendor reports and commercial providers themselves — in products like intrusion detection and prevention systems (IDPSs), secure web gateway (SWG), secure email gateway (SEG) and enterprise firewalls.

In a threat-intelligence-specific example, users may seek domain intelligence to help ascertain whether users are accessing a domain that is less than 30 days old. Domains that are this “young” are far more likely to be malicious. Another example involves an SIEM resource having an actively curated list of malicious domain names in its correlation engine — looking for any activity of those domains in your organization. Upstream threat intelligence (TI) providers can ensure that this DNS watchlist is both effective and well-curated with multiple upstream sources combined in one place for dispersion into your existing product ecosystem.
End-user organizations today are facing a long-term and sustained trend of phishing attacks. These campaigns don’t happen in isolation, but require planning (including accounting for components of the attack that are public knowledge prior to their execution). One use case that threat intelligence providers can perform is to monitor for the registration of potential phishing domains as they are registered by known bad actors or hosted in known bad places on the internet. Many threat actors that use so-called bulletproof hosters still need their malicious domains to propagate through the rest of the internet for their domains to work for average internet users. This process happens in the open and is a security monitoring use case worthy of implementing.

Use DNS for Activity Monitoring and Analytics

At a minimum, monitoring your DNS logs is a rich source of telemetry documenting activity in your environment that is helpful for security use cases. Is monitoring DNS appropriate for every IT or security operations team? No, because it requires the capacity to capture, store and analyze DNS logs, which can be voluminous, even in smaller organizations. Even if you have a log management tool or SIEM solution, you may not have the capacity to store DNS logs for longer periods without licensing implications. Regardless, at least some DNS storage in a SIEM should be possible as it is a relatively efficient and effective source of telemetry to have access to and does not take up much space. However, increasingly SIEM solutions, and some log management tools, are pricing themselves not based on the velocity or volume of logs collected, but per asset or employee.

If you have a tool that is priced per asset or employee, you likely have available capacity to start collecting DNS logs for security use cases.

Analysis based on DNS is a bit trickier, but several SIEM solutions (see Critical Capabilities for Security Information and Event Management) and some IDPS have analytics like domain generation algorithms (DGA) that monitor DNS traffic and logs for anomalous-looking domain names based on various characteristics (naming structure, registration history and location). This allows them to indicate when there is an active threat in your environment.

A number of SIEM solutions that offer user and entity behaviour analytics (UEBA) may also look for behavioural anomalies in DNS traffic, including by IP address, domain, time of access, and the size of the DNS requests (e.g., the covert data exfiltration use case). Most SIEM solutions also support analyzing logs, including DNS, against threat intelligence feeds, to look for hits. Some log management tools that support security use cases also offer these features (see Use Central Log Management for Security Operations Use Cases).

Additionally, threat-hunting use cases rely on strong signals that can be reviewed over longer time epoch’s to determine if a host was compromised in the past or not. DNS is one of these strong signals,
and also an efficient method of event telemetry storage. This is due to its ability to not take up much space in tooling like a SIEM or EDR tool and therefore support rapid searching use cases.

Use DNS Services to Protect Work-From-Home Employees

Many vendors offer managed DNS services for enterprises — most are paid, but some have free prosumer options as well. A key benefit of using these services is that they can be implemented in minutes since there is no software or hardware to install once the service has been configured.

Alternatively, updates to end-user device configurations can be pushed to change the DNS servers on an endpoint, or users can be given instructions to manually change them in the worst case scenario.

Other benefits include:

- Central management of a DNS policy.
- A single point for visibility of threats targeting those users’ devices.
- Access to DNS logs for collection, analysis and storage.
- Security and privacy from tracking of DNS name requests.

It should be noted that there is a relatively large number of product categories that support DNS security use cases today. Firewall, IDPS/network detection and response (NDR), SIEM, EPP/EDR, SWG all have DNS security capabilities. We recommend you investigate whether your current vendors in these categories can address DNS use cases, so that you can avoid needing to acquire a new product.

Securing IoT and Operational Security Assets

There are already billions of “things” connected to the internet inside and outside of enterprise networks. These devices heavily rely on connecting to a network in order to function, primarily after making DNS requests. DNS can play a critical role here regardless of whether the request is made by a small inexpensive IoT device or a very expensive piece of operational technology. In essence, this exploits the same use cases mentioned above, but is applied to a different class of assets. Allow and deny enforcement, application control, DNS host isolation, threat hunting and DNS analytics (among other capabilities) are all very useful use cases for IoT devices on which agent-based security solutions cannot be installed. For these types of assets, DNS (like logging) is often the only thing on these hosts that we can use for security enforcement.

Recommended by the Authors

Security Operations Primer for 2021

Evidence

1 DNS Queries Over HTTPS (DoH), IETF Datatracker.
2 Top 11 Tips for Cyber Security, CERT NZ.

3 Essential Eight Explained, Australian Cyber Security Centre.

4 NIST Offers Guidance on Using Technology to Prevent Intrusions, Malware, The National Institute of Standards and Technology (NIST).